La valutazione del Red Team da Seqrite Services ha prodotto risultati significativi per un importante istituto finanziario

Informazioni sul cliente

Questo cliente Seqrite Services è una grande banca del settore privato che, oltre a offrire una vasta gamma di servizi finanziari, include anche servizi personali, aziendali e di gestione della ricchezza.

Perché il Red Team è necessario

Le sfide lungo il percorso di una nota istituzione finanziaria sono diverse. Ogni pezzo di informazione, disponibile fisicamente o digitalmente, è di massima riservatezza. Molte responsabilità, azioni e decisioni sono eseguite all'interno dell'organizzazione con i tipi di dati menzionati e la loro sicurezza. La valutazione Red Team fornisce la comprensione pratica di come un attaccante può ottenere l'accesso non autorizzato a informazioni sensibili che portano a violazioni dei dati e ad altre perdite.

La nostra strategia

La valutazione Red Team è la nostra offerta di punta e la più completa. Non è un approccio unico per tutti; personalizziamo la nostra strategia come unica nel suo genere tenendo conto delle esigenze e dei piani dell'organizzazione. Nella riunione di avvio abbiamo deciso insieme l'ambito, gli obiettivi e i parametri della matrice di successo e abbiamo spiegato ai Game Masters le nostre attività, metodologie, tempi e ruoli del team per la valutazione.

Molteplici Vettori di Attacco

Il Red Team rivela opportunità reali che sfruttano i buchi e compromettono tutti gli aspetti di un'organizzazione. Seqrite Services ha utilizzato una varietà di tecniche per ottenere l'accesso ai loro dati sensibili. Sulla base degli sforzi di ricognizione e dei percorsi di attacco, il nostro Red Team ha eseguito con successo ciascun attacco, che ha fornito preziose informazioni. Le attività seguenti sono state eseguite in questo attacco multifaccettato per misurare quanto bene la rete, le applicazioni, i controlli di sicurezza fisica e le persone della banca possano resistere a un attacco in tempo reale.

1. Open source intelligence (OSINT) e Tecniche di Monitoraggio Darknet

- Esaminata l'esposizione delle informazioni della banca e dei suoi dipendenti tramite OSINT e monitoraggio Darknet.
- Sfruttato queste informazioni per accedere direttamente ai dipendenti, ottenere informazioni altamente sensibili come i PAN Card di 4 CxOs

2. Penetrazione di Applicazioni Web e Mobile

- Eseguiti test automatici e manuali di applicazioni web che hanno stimolato le minacce attuali insieme a pivoting e post-exploitation.
- Compromessa l'applicazione web principale dell'organizzazione scrivendo un exploit personalizzato.
- Ottero con successo l'accesso remoto al loro server web sfruttando vulnerabilità come SQL Injection e Cross site scripting (XSS)
- Eseguiti test dinamici e statici delle applicazioni mobili per tutte le piattaforme
- Eseguiti test di bypass proxy e validati i controlli di sicurezza interni ed esterni.
- Valutata la sicurezza sia in termini di vulnerabilità tecniche sia di difetti di logica di business.
- Verifica reale delle loro capacità di risposta agli incidenti e di rilevamento.

3. Test di Intrusione di Rete Interne ed Esterne

- Recon- server web non configurati correttamente, credenziali trapelate oltre ai dettagli convenzionali
- Ottenere accesso shell ai server critici aziendali compromettendo i punti Wi-Fi interni/esterni.
- Condotto PT su rete esposta pubblicamente così come sulla rete interna
- Valutata la postura di sicurezza di router, firewall, IDS e altri dispositivi di sicurezza.
- Verificate possibili cattive configurazioni e vulnerabilità correlate con le applicazioni presenti nella rete.

4. Attacchi di Ingegneria Sociale

- Compromesso cinque (5) account email utente / password e altri dettagli come ID dipendente, reparto, ecc. attraverso diverse tecniche di social engineering come:
    - Phishing / Spear Phishing
    - Vishing / Chiamata Diretta
    - SmiShing / Evil Twin
    - USB Baiting
    - Assunzione di conversazioni/ Riunione off-site

5. Breccia nella Sicurezza Fisica

- Condotto PT fisico per Data Centre, Ufficio Aziendale e Ufficio di Filiale
- Analisi dei punti di transito vulnerabili
- Inseguimento / bypass del controllo accessi e ottenimento di accesso a dispositivi e reti interne
- Elencate le contromisure di sicurezza fisica
- Valutazione della consapevolezza dalla Guardia di Sicurezza al C-Suite.

Risultati e Conclusioni della Valutazione Red Team

La valutazione Red Team eseguita da Seqrite Services è stata altamente riuscita e ha prodotto un insieme significativo di risultati. Durante i test di intrusione fisica, la consapevolezza della sicurezza, dai vigilantes al C-suite, è stata valutata e la maggior parte di loro non ha seguito l'igiene di sicurezza di base; poiché il nostro team è riuscito ad ottenere l'accesso ai sistemi, walkthrough del piano senza controllo, documenti sensibili, baiting USB e molto altro.La risposta agli incidenti è stata lenta e inefficace, permettendo al nostro team di andarsene senza rimproveri.

Le informazioni raccolte tramite intelligence dalle fonti aperte e monitoraggio darknet hanno rivelato la mancanza di consapevolezza della sicurezza da parte di molti dirigenti a livello esecutivo, i quali non proteggono adeguatamente la loro impronta digitale; di conseguenza abbiamo ottenuto la carta PAN di quattro CxOs, portali intranet della banca e risposte a e-mail personalizzate e fraudolente, nonché chiamate telefoniche, tutte eseguite dai Seqrite Services.

I test di intrusione hanno rivelato una serie di vulnerabilità nelle applicazioni operative, che va dalle applicazioni web alle applicazioni mobili, provocando una causa principale: mancanza di aderenza alle politiche di sicurezza che lasciano la banca vulnerabile agli attacchi da parte di qualsiasi membro del team Seqrite Services che esegua questa attività.

Seqrite Services si è assicurato che nessun dettaglio fosse trascurato e ha fornito raccomandazioni per tutti i problemi per garantire che non rimanga alcun dubbio riguardo alle pratiche corrette per chiudere queste lacune di sicurezza, e continuerà a farlo in futuro in quanto loro partner di sicurezza di fiducia.

> "Il Red Team di Seqrite Services ha dato il massimo impegno affinché il lavoro fosse completato nei tempi e nei costi previsti. La qualità del prodotto finale è risultata superiore alle specifiche. Siamo stati particolarmente colpiti dal loro approccio professionale nel gestire questioni potenzialmente sensibili nelle organizzazioni studiati e dalla loro capacità di coinvolgere tutti gli stakeholder. Sono stati molto proattivi e reattivi nelle comunicazioni sui progressi e sui problemi durante tutto il lavoro. Di conseguenza, non vediamo l'ora di lavorare di nuovo con Red Team in futuro e non esiteremmo a raccomandarli per progetti simili."
>
> - CISO, Banca